REMARKS

I. INTRODUCTION

In response to the Office Action dated July 17, 2007, the claims have not been amended. Claims 1-3, 5-15, 17-27, 29-38, 40-50, and 52-63 remain in the application. Re-consideration of the application is requested.

II. NOTICE OF RELATED CASES

Applicants note that page 1 of the originally filed specification identifies several cases related to the present application. Applicants encourage the Examiner to review the file history of such related cases to make an independent determination regarding the relevance of any correspondence between the Applicant and Patent Office (e.g., Office Actions, Responses, etc.).

II. SUMMARY OF THE INVENTION

Independent claims 1, 12, 24, 35, and 47 are generally directed to controlling access to digital services (page 1, lines 19-21). More specifically, digital services are processed in a control center, uplinked to a satellite, and received at a subscriber receiver station where they are processed by a conditional access module (CAM) (page 4, lines 16-23; page 10, line 28-page 11, line 10; FIGs. 1, 5, and 6).

The claims further provide specific limitations relating to the CAM. In this regard, the CAM has a system bus (page 14, line 26, FIG. 6), and a plurality of physically separate and independently controlled nonvolatile memory components (page 14, line 21-page 15, line 2; FIG. 6; page 15, lines 15-28; FIG. 7). Access control to the digital services is distributed among the multiple nonvolatile memory components (page 14, lines 16-20; FIG. 6 and 7 [700] and [702]). In addition, a microprocessor is coupled to each of the nonvolatile memory components (page 15, lines 3-6; page 16, lines 6-8; FIG. 7 [704]) . The microprocessor has various capabilities including the ability to use state information in the memory components to provide desired functionality and enforce a security policy for accessing the digital services (page 16, lines 8-21; FIG. 7). The single microprocessor further controls each of the nonvolatile memory components (page 16, lines 8-21; FIG. 7). Further, the memory components each have separate memory access and control restrictions (page 16, lines 11-12; FIG. 6 and 7).

Accordingly, as set forth above, not only are each of the multiple nonvolatile memory components independently controlled, but they have separate memory access and control restrictions while being controlled by the same microprocessor.

III. DOUBLE PATENTING REJECTION

On page (13), paragraphs (1)-(2) of the Office Action, claims 1, 12, 24, 35, and 47 of instant application 10/085,331 are provisionally rejected under the judicially created doctrine of obviousness-type double patenting as being unpatentable over claims 1, 8, 15, and 22 of copending Application No. 10/085,920.

Applicants note that the subject matter of the copending application and the present application may change thereby obviating the need for the submission of a terminal disclaimer. Applicants may be willing to submit a terminal disclaimer should one become necessary. However, at this time, Applicants traverse the rejection while reserving the right to submit a terminal disclaimer at a later date and upon the determination of allowable subject matter.

III. PRIOR ART REJECTIONS

On pages (4)-(11) of the Office Action, claims 1-3, 5-15, 17-27, 29-38, 40-50 and 52-63 were rejected under 35 U.S.C. §103(a) as being obvious in view of the combination of Cohen et al., U.S. Patent 5,282,249 (Cohen) and Kocher, U.S. Patent 6,289,455 (Kocher). Applicants respectfully traverse these rejections.

Specifically, claim 1, 12, 24, 35 and 47 was rejected as follows:

> Regarding claim 1, Cohen teach and describe a system for controlling access to digital services comprising:
>
> (a) a control center configured to coordinate and provide digital services;
>
> (b) an uplink center configured to receive the digital services from the control center and transmit the digital services to a satellite (Fig. 1/1 Item 20);
>
> (c) the satellite configured to:
>
> (i) receive the digital services from the uplink center (Fig. 1/2 Item 22);
>
> (ii) process the digital services (Fig. 1/2 Item 22); and
>
> (iii) transmit the digital services to a subscriber receiver station (Fig. 1/2 Item 24);
>
> (d) the subscriber receiver station configured to:
>
> (i) receive the digital services from the satellite (Fig. 1/2 Item 26);
>
> (ii) control access to the digital services through an integrated receiver/decoder (IRD) (Fig. 1/2 Item 30);
>
> (e) a conditional access module (CAM) communicatively coupled to the (IRD) (Fig. 1/2 Item 32) [col. 4 line 12 to line 66],

Cohen do not disclose the CAM comprising nonvolatile protected memory component having state information to enforce desired functionality.

However, Kocher disclose the CAM (Fig. 2 Item 225) comprising:

(i) a system bus;

(ii) a plurality of physically separate and independently controlled nonvolatile memory components (col. 21 line 13 to line 15), wherein access control to the digital services is distributed among the nonvolatile memory components (col. 21 line 2 to col. 22 line 25); and

(iii) a microprocessor communicatively coupled to the nonvolatile memory components, wherein separate and independent attacks must be conducted on each nonvolatile memory component to gain unauthorized access to the digital services; and a microprocessor communicatively coupled to the nonvolatile memory, wherein the microprocessor is configured to use state information in the nonvolatile memory components to provide desired functionality and enforce one or more security policies for accessing the digital services, and wherein the microprocessor controls each of the plurality of nonvolatile memory components and each nonvolatile memory component has separate memory access and control restrictions (col. 10 line 5 to line 47, col. 5 line 55 to col. 6 line 3, and col. 24 line 10 to line 30).

Kocher is analogous art because it discusses a method and apparatus for preventing piracy of digital content including the use of a smart card. Therefore, it would have been obvious to one ordinary skilled in the art at the time of invention to include the teaches and features of CAM found in Kocher in the smart card used by Cohen, to control access to the broadcast data, because Kocher's method of protected memory of monitored data by using state information would not only promote security structure in the system of Cohen during receiving and distributing digital content (Kocher: Fig. 1, col. 5 line 55 to line 56, and col. 6 line 65 to line 67) but will also provide safeguards against attempt by unauthorized person to breach security of system.

Applicant traverses the above rejections for one or more of the following reasons:

(1) Neither Cohen nor Kocher teach, disclose or suggest a single microprocessor that controls multiple nonvolatile memory components that are physically separate and independently controlled; and

(2) Neither Cohen nor Kocher teach, disclose or suggest a single microprocessor that controls multiple nonvolatile memory components with separate memory access control restrictions.

The Office Action admits Cohen's lack of teaching of multiple nonvolatile memory components as claimed. To teach these elements of the claims, the Office Action relies on Kocher col. 21, line 13 to col. 22 line 25 and col. 24, line 10 to line 30. Applicants respectfully disagree with and traverse such rejections. Namely, these portions of Kocher completely fail to describe multiple nonvolatile memory components organized in the manner claimed. Instead, Kocher merely describes multiple microprocessors that each may have its own RAM, ROM, and EEPROM (see col. 21, lines 34-40). However, the ability for a single microprocessor to independently control separate nonvolatile memory components is not taught or disclosed, explicitly or implicitly, in Kocher. The use of multiple nonvolatile memory components as claimed provides significant advantages over the prior art including Kocher. Paragraph [0062] of the application as filed describes some of such advantages:

> [0062] FIG. 6 illustrates the architecture of a CAM 512 in accordance with one or more embodiments of the invention. The CAM 512 contains a microprocessor 602, volatile memory components 604 (e.g., random access memory [RAM]), a plurality of nonvolatile memory components 606 (e.g., electrical erasable programmable read only memory [EEPROM], erasable programmable read only memory [EPROM], or batter packed RAM), and a system input/output module 608, all of which are communicatively coupled to a system bus 610. As illustrated, a plurality of nonvolatile memory components 606 are utilized. Using this approach, each nonvolatile memory component 606 has separate memory access control restrictions and may implement entirely unique memory access control logic. This forces an intruder to embark on multiple separate attacks to compromise each memory component 606.

As can be seen, such an approach forces an intruder to attempt multiple separate attacks in order to access each separate memory component and gain access to the digital services. However, Kocher does not even remotely allude to such a benefit or capability. Instead, Kocher merely describes two microprocessors – one serves as an interface control processor (ICP) that communicates with a second processor that is a cryptofirewall that controls access to a protected memory (see col. 7, lines 54-60 and col. 21, lines 34-54). However, such a teaching completely and totally fails to describe or suggest a single microprocessor that access multiple nonvolatile memory components that are not in protected memory.

Applicants further note that claims 3, 24, 37, and 49 provide a limitation for a custom logic block that is further described in copending patent applications. It is noted that the custom logic block controls access to memory. However, the multiple nonvolatile memories of the present invention are not controlled by the custom logic block. FIG. 6 of the present invention illustrates the multiple nonvolatile memory components of the system as claimed. There are clearly significant, distinguishable, and nonobvious differences from the system of FIG. 6 as claimed and Kocher (and/or the combination of Kocher with Cohen).

In response to the above, the final Office Action provides that Kocher teaches a system and method that relates to a number of selectable and portable executing devices, each being operatively associated with any one receiving descrambler and each executing identical operations to generate a seed for use by the associated receiving descrambler to enable the receiving descrambler to descramble the broadcast. The final Office Action relies on Kocher Fig. 1-2, col. 4, line 12-66, col 21, line 2-col. 22, line 25. Further the Action provides:

> In particular, fixed data and code are stored in ROM, temporary data (and possibly code) are stored in RAM, and additional code and/or data are stored in EEPROM which can be modified by processor. Also attached to bus is CryptoFirewall, a specialized cryptographic processing unit which regulates and cryptographically modifies data written to or read from protected memory (Fig. 2, col. 9, line 29 to line 59).

Applicants note that RAM is not nonvolatile memory. Further, the CryptoFirewall contains a processing unit itself and merely modifies data written to or read from protected memory (see col. 9, lines 37-41).

The claims provide that access control to the digital services is distributed among the multiple nonvolatile memory components. Further, separate and independent attacks must be conducted on each of the nonvolatile memory components to gain unauthorized access to the digital services. Thus, rather than being able to attack one nonvolatile memory unit and gaining access to all of the digital services, the present invention provides that all of the nonvolatile memory components must be accessed to gain access to the digital services. Merely accessing one component is insufficient. Applicants again direct the attention of the patent office to paragraphs [0059]-[0068] of the originally filed specification. For example, paragraph [0061] provides as follows:

> **[0061]** To avoid this method of attack, access to the nonvolatile memory components is distributed among several physically separate and independently controlled nonvolatile memory components. Using this approach, it may not be possible to compromise one nonvolatile memory component and march through all memory address locations that reside other memory components. Only the attacked memory component is compromised.

Similarly, paragraph [0065] provides as follows:

> **[0065]** There are many advantages to using a plurality of nonvolatile memory components 606 in a CAM 512. For example, the nonvolatile memory components 606 have physically separate address spaces and physical locations on the die. Further, each nonvolatile memory component 606 would have to be attacked and compromised separately. Separate memory control units can be implemented allowing each control unit to be uniquely customized and tailored to the specific memory module 606 being protected. This design requires each nonvolatile memory component 606 to be attacked separately and individually. Therefore, the entire chip can withstand substantial external attack through the system I/O module 608. Accordingly, the use of such a plurality of nonvolatile memory components enables the protection of video, audio, broadband, and data/digital services reception.

Lastly, paragraph [0068] provides as follows:

> **[0004]** At step 706, digital services are accessed using the nonvolatile memory components 606 to provide desired functionality and enforce security policies for the access. Using the identified configuration with a plurality of nonvolatile memory components 606, if unauthorized access is attempted, separate and independent attacks must be conducted on each nonvolatile memory component 606.

As can be seen, the invention as claimed provides more than merely reciting multiple nonvolatile memory components. Instead, the multiple components control access to the digital services and provide for a more secure environment. Further, the access control is distributed across the multiple components. Thus, even if one component were compromised, the access to the digital services would not be compromised without also gaining access to the remaining components. The various teachings of Kocher do not even remotely refer to or resemble such an architecture or secure system as claimed. Further, the final Office Action fails to describe how Kocher teaches such explicit and detailed claim limitations.

Again, while Kocher teaches (in FIG. 1 and 2), a memory connected to a microprocessor (Fig. 1), and ROM245 and EEPROM 255 connected to a bus 240 (Fig. 2), neither of the figures depict the limitations of the claims. Further, Kocher's specification also fails to describe the claim limitations. What is notoriously lacking from Kocher is any description of distributing access control to digital services across multiple nonvolatile memory components that have to be separately attacked in order to gain access to the digital services (as claimed). Instead, Kocher merely refers to the use of ROM 245 and EEPROM 255 in addition to the use of protected memory 265 via cryptofirewall 260. Such a use of the cryptofirewall 260 is irrelevant to the present claims since a separate microprocessor exists within the cryptofirewall as described above (while the present claims require a single microprocessor). Further, the other components do not control access to digital services. Thus, Kocher does not and cannot teach the invention as claimed.

In response to the above arguments, the prior Office Action merely provides that a cryptographic unit transforms data from the microprocessor and uses memory contents and the transformation result is utilized to decode digital content. The Action continues and provides that the CRU includes an interface control processor (ICP) that is responsible for communication with a playback device and includes several types of memory connected to the ICP via bus. The Action states that in particular, fixed data and code are stored in ROM, temporary data is stored in RAM, and additional code and/or data is stored in EEPROM that can be modified by the processor. Further, the Action provides that a cryptofirewall and cryptographic processing unit are attached to the bus and are used to regulate and cryptographically modify data written to or read from protected memory.

However, what is missing from such a description is a plurality of independently controlled nonvolatile memory components wherein access control to the digital services is distributed among the components. Firstly, RAM is irrelevant since it is not nonvolatile memory. Secondly, the access control to the digital services is NOT distributed across Kocher's ROM and EEPROM.

The claim limitations relating to distribution of access control are further set expressly in the claims that provide that separate and independent attacks must be conducted on each nonvolatile memory component to gain access to the digital services. Further, state information in the nonvolatile memory components is used by the microprocessor to enforce security policies for accessing the digital services. In addition, the single microprocessor controls each of the nonvolatile memory components via separate memory access and control restrictions. Again, Kocher fails to provide or even remotely allude to such a teaching. Instead, Kocher describes for storing fixed data and code in ROM and additional code and/or data in EEPROM. However, there is no mention or description that such code and/or data is part of an access control system that has been distributed across the ROM and EEPROM. Nor is there any mention or description, explicit or implicit, that to gain unauthorized access to the digital services, separate and independent attacks must be conducted on both the ROM and EEPROM.

Instead of even alluding to the claimed limitations, Kocher provides for utilizing two microprocessors that each have their own RAM, ROM and EEPROM (see col. 21, lines 35-39). In this regard, one microprocessor serves as the ICP and communicates with a second microprocessor which is the cryptofirewall. However, contrary to that set forth in the claims, Kocher has different memories for each microprocessor. Further and more importantly, the access control to the digital services is not distributed across multiple memories that are controlled by a single microprocessor (as claimed).

In view of the above, it is noted that the Office Action ignores the claim limitations relating to the distribution of access control. The Office Action further ignores the explicit claim limitations providing that separate and independent attacks must be conducted on each nonvolatile component to gain unauthorized access. Under MPEP §2142 and 2143.03 "To establish *prima facie* obviousness of a claimed invention, all the claim limitations must be taught or suggested by the prior art. *In re Royka*, 490 F.2d 981, 180 USPQ 580 (CCPA 1974). "All words in a claim must be considered in judging the patentability of that claim against the prior art." *In re Wilson*, 424 F.2d 1382, 1385, 165 USPQ 494, 496 (CCPA 1970)." The Office Action has failed to address all of the claim limitations or has merely summarily rejected them without stating where either reference teaches such a limitation.

The Office Action groups together all of the limitations relating to the nonvolatile memory components into one paragraph and summarily recites Kocher, col. 10, lines 5 to 47, col. 5, line 55 to col. 6, line 3, and col. 24, line 10 to line 30. Col. 10, lines 5-47 merely describe a protected memory having EEPROM and the use of different keys. However, the distribution of access control is neither described or alluded to. Col. 5, line 55 to col. 6, line 3 merely describes a summary of Kocher's security system that includes a microprocessor, a memory, a cryptographic unit connected between the microprocessor and the memory that protects the memory, and a device key accessible by the cryptographic unit and inaccessible by the microprocessor such that the cryptographic unit uses the contents of the memory to transform a data value received from the microprocessor that is required to decode the digital content. However, once again, such a description fails to describe the distribution of access control across multiple nonvolatile memory components wherein separate and independent attacks of each component are required to gain unauthorized access to the digital services (as claimed).

Col. 24, lines 10-30 describe how a physical invasive attack can provide the ability to read from and/or write to the protected memory. The text further describes that such reading/writing provides no particular value, since the keys stored in the protected memory are not useful without the algorithms that are implemented in the cryptographic unit. The text then describes that a proper functioning cryptofirewall is still required to process the values from the protected memory into content decryption keys. The text concludes by stating: "AS A RESULT, THE ATTACKER'S WORK MODIFYING ONE CHIP CAN YIELD ONE FULLY-FUNCTIONAL PIRATE DEVICE, BUT SHOULD NOT LEAD TO A GENERAL ATTACK THAT CAN BE MARKETED ON A WIDE SCALE". As can be seen, rather than preventing access to digital services, Kocher explicitly teaches that a pirate device can be created merely by accessing the protected memory. Such a teaching would actually serve to teach away from the present invention since such a device would not require independent and separate attacks of each nonvolatile memory component. In addition, such a teaching completely and wholly fails to describe distributing access control across multiple nonvolatile memory components that are controlled by a single microprocessor yet has separate memory access and control restrictions. Again, Kocher fails to describe or suggest the explicit and detail claim limitations that are set forth in the present claims.

Instead, the mere interaction between a CRU and microprocessor are described without any reference or description to the limitations set forth in the claims and described herein.

In addition to the above, Applicants note that the other cited references also fails to cure Kocher's deficiencies.

Applicants also note that previously added dependent claims 59-63 provide that at least one of the plurality of physically separate and independently controlled nonvolatile memory components is protected from modification such that the protected nonvolatile memory component is read only, and access to the protected nonvolatile memory component is isolated. Further, these claims provide that a microprocessor's unprotected nonvolatile memory component and the protected nonvolatile memory component use physical and logical address ranges that are the same. Such a teaching and use of the same physical and logical address ranges across multiple different nonvolatile memory components is neither taught nor suggested by any of the cited references.

Moreover, the various elements of Applicants' claimed invention together provide operational advantages over Cohen and Kocher. In addition, Applicants' invention solves problems not recognized by Cohen and Kocher.

In response to the above arguments, the final Office Action essentially repeats the prior rejections. The final Action again repeats that attached to the bus is a cryptofirewall, that is a specialized cryptographic processing unit which regulates and cryptographically modifies data written to or read from protected memory. Again, dependent claims 59-63 provide for protected memory and clearly distinguish such memory from the other multiple nonvolatile memory components that are controlled by a single microprocessor. In this regard, Kocher explicitly recites multiple processors rather than the single microprocessor that controls multiple nonvolatile memory components all of which must be accessed independently in order to gain access to digital services as claimed. Regardless of whether Kocher recites the ability to prevent unauthorized access to digital services, the present claims provide for more than merely preventing access - they explicitly recite specific limitations that are used to prevent such access. Namely, the single microprocessor accesses multiple nonvolatile memory components:

> "a plurality of physically separate and independently controlled nonvolatile memory components, wherein access control to the digital services is distributed among the nonvolatile memory components wherein separate and independent attacks must be

conducted on each nonvolatile memory component to gain unauthorized access to the digital services;"

Again, such claim limitations are not even remotely hinted at or suggested in either the text or Figures of Kocher or Cohen.

Thus, Applicants submit that independent claims 1, 12, 24, 35 and 47 are allowable over Cohen and Kocher. Further, dependent claims 2, 3, 5-11, 13-15, 17-23, 25-27, 29-34, 36-38, 40-46, 48-50 and 52-63 are submitted to be allowable over Cohen and Kocher in the same manner, because they are dependent on independent claims 1, 12, 24, 35 and 47, respectively, and because they contain all the limitations of the independent claims. In addition, dependent claims 2, 3, 5-11, 13-15, 17-23, 25-27, 29-34, 36-38, 40-46, 48-50 and 52-63 recite additional novel elements not shown by Cohen and Kocher.

IV. CONCLUSION

In view of the above, it is submitted that this application is now in good order for allowance and such allowance is respectfully solicited. Should the Examiner believe minor matters still remain that can be resolved in a telephone interview, the Examiner is urged to call Applicants' undersigned attorney.

Respectfully submitted,

Date: September 14, 2007

By:
Name: Georgann S. Grunebach
Registration No. 33,179

The DIRECTV Group, Inc.
CA / LA1 / A109
P.O. Box 956
2230 E. Imperial Highway
El Segundo, CA 90245-0956